



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/694,416 90/005776 90/005733 ⁵⁹⁰	10/20/2000 08/22/2005	Thomas Collins	20206-014(PT-TA-410)	1055
HEWLETT-PACKARD COMPANY Intellectual Property Administration P.O. Box 272400 Fort Collins, CO 80527-2400			EXAMINER	
			SMITHERS, MATTHEW	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 08/22/2005
08/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.



UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

Address: ASSISTANT COMMISSIONER FOR PATENTS

Washington, D.C. 20231

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
---------------------------------	-------------	---	---------------------

90/005,733

07/28/2000

5848159

90/005,733
09/05/776
09/16/94, 4.16

Patent Administrator

TESTA, HURWITZ & THIBEAULT, LLLP

125 High Street

Boston, MA 02110

EXAMINER

Smithers, Matthew B.

ART UNIT

PAPER

2137

DATE MAILED: 08/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

CC: HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

Office Action Summary

Application No.

90/005,733 ; 90/005, 776
09/694,416

Applicant(s)

COLLINS ET AL.

Examiner

Matthew B. Smithers

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 28 June 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-6,9-12 and 14-61 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-6,9-12,14-31,34-36,38-44 and 50-61 is/are rejected.
- 7) ☒ Claim(s) 32,33,37 and 45-49 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>1/7/05</u> . | 6) <input type="checkbox"/> Other: _____ |

Art Unit: 2137

DETAILED ACTION

Status of Claims

Claims 1-6, 9-12, and 47 were amended.

Claims 7, 8, and 13 were canceled.

Claims 1-6, 9-12 and 14-61 remain pending.

Response to Arguments

Applicant's arguments, see pages 31-40, filed June 28, 2005, with respect to the rejection(s) of claim(s) 1-61 under 35 USC 112 have been fully considered and are persuasive. Applicant's arguments, see pages 31-40, filed June 28, 2005, with respect to the rejection(s) of claim(s) 1-7, 9-61 under 35 U.S.C. 103(a) as being unpatentable over Rivest et. al. (US 4,405,829 A) and further in view of Rivest et. al., "A Method for Obtaining Digital Signatures and Public-key Cryptosystem", Communications of the ACM, 21(2) February 1978, and further in view of Knuth, "The Art of Computer Programming vol. 2 page 179, have been fully considered and are persuasive. Applicant's arguments, see pages 31-40, filed June 28, 2005, with respect to the rejection(s) of claim(s) 1-6, 9-12, 14-31, 34-36, 38-44, and 50-61 under 35 U.S.C. 103(a) as being unpatentable over Nemo, "RSA Moduli Should Have 3 Prime Factors", and further in view of Rivest et. al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystem" have been fully considered and are persuasive. With respect to the

Art Unit: 2137

rejection of the claims using Captain Nemo, a further search to determine the existence of the magazine "Scientific Bulgaria" was conducted, however the magazine could not be found. Therefore the rejection has been withdrawn at this time.

Applicant's arguments filed June 28, 2005, concerning the rejection of Vanstone and Zuccherato, the rejection of Itakura and Nakamura, and the rejection of Slavin, have been fully considered but they are not persuasive. For the rejection of Vanstone and the rejection of Itakura, applicant argues the references fail to teach random and distinct prime numbers. The examiner respectfully disagrees with the arguments and asserts the references do show prime numbers that are distinct and random. In Vanstone, the prime numbers are generated by first choosing a random a_1 , a_2 , and a_3 , respectively, which in turn produces randomly distinct prime numbers. In Itakura, each of the primes p , q , and r are arbitrarily selected (random) and none of them have a specified relationship between each other (distinctness). Therefore, the examiner believes the prime numbers in each of the references is distinct and random. The examiner maintains the rejections of Vanstone and Itakura (see previous office action dated 07 October 2004).

Regarding applicant's arguments concerning the Slavin reference, the examiner contends applicant has failed to point out the distinctions between the reference and the claimed invention. The examiner believes the reference anticipates the claimed

Art Unit: 2137

invention should have been cited under 102(e) instead of a 102(a) in the previous office action. The correct citation and application of the prior art (Slavin) is given below.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-6, 9-12, 14-31, 34-36, 38-44, and 50-61 are rejected under 35

U.S.C. 102(e) as being anticipated by U.S. 5,974,151 granted to Slavin.

Salvin discloses a method of encrypted communication (Abstract) using four prime RSA $n = p_1 \times q_1 \times p_2 \times q_2$, in which the four primes are selected at random and all of which all are different (i.e. distinct) values (Column 7, lines 35-67; . . . The preferred embodiment follows the steps : 1. Instead of two primes as used in the RSA technique, we use four randomly selected primes, p_1, q_1, p_2, q_2 , all of different values . . .) and corresponding public and private keys e and d (see figure 3, Column 4, lines 31-38 applied to a network with a plurality of users (Figure 1). Salvin further discloses the use of the CRT to speed up the 4 prime decryption (Column 9, lines 44-47) whose speed is

Art Unit: 2137

inherent from the breaking up the modular exponentiation into smaller primes and parallel subtasks.

Allowable Subject Matter

Claims 32-33, 37 and 45-49 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Art Unit: 2137

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B. Smithers whose telephone number is (571) 272-3876. The examiner can normally be reached on Monday-Friday (8:00-4:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Matthew B Smithers
Primary Examiner
Art Unit 2137